

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Brian P. Prive, depose and state the following:

Introduction and Affiant Background

1. I have been a law enforcement officer for over 14 years and have been a United States Postal Inspector since August of 2022. I am currently assigned to the Boston Division, Providence, Rhode Island, domicile of the United States Postal Inspection Service (USPIS). I am responsible for the investigation of various crimes relating to the United States Mail including, but not limited to, mail theft, bank fraud, identity theft, and mail fraud. Prior to my appointment as a Postal Inspector, I was a law enforcement officer with the United States Department of Veterans Affairs Police for approximately 13 years. I have training and experience in conducting investigations of crimes that adversely affect, or fraudulently use, the United States Mail and the United States Postal Service (USPS); as well as training and experience in investigations of wire fraud, bank fraud, check fraud, and identify theft. I have a BA in Political Science from Bridgewater State University and a JD from Suffolk University Law School.

2. I submit this affidavit in support of an Applications for Search Warrants pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a search of the following person and location:

- a. The person of JAMAL MANSARAY, YOB 1989 (the “SUBJECT PERSON”), as more particularly described in Attachment A-1 for the items described in Attachment B, at whatever location he is found, regardless of MANSARAY’s location or proximity to SUBJECT PREMISES, including any cellular telephones or digital storage devices he may have on his person; and
- b. The premises (the current residence of MANSARAY) at 180 Waterman Avenue, Apt. [REDACTED], North Providence, Rhode Island 02911 (the “SUBJECT PREMISES”), as more particularly described in Attachment A-2, for the items described in Attachment B;

3. As set forth below, there is probable cause to believe that located on and with the SUBJECT PERSON and within the SUBJECT PREMISES are evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1344 (bank fraud), 18 U.S.C. § 1029

(access device fraud), 18 U.S.C. § 1028A (aggravated identify theft), and 18 U.S.C. § 1708 (theft or receipt of stolen mail matter).

4. The facts set forth in the Affidavit are based on my personal observations, my training and experience, information obtained from other Inspectors, agents, officers, witnesses, and records obtained during the course of the investigation. Because this affidavit is being submitted for the limited purpose of showing probable cause for the issuance of the requested arrest warrant and complaint, and search and seizure warrants, I have not included each and every fact known to me and other law enforcement officers involved in this investigation. Rather, I have included only those facts that I believe are necessary to establish probable cause for the issuance of the requested complaint and arrest, search, and seizure warrants.

PROBABLE CAUSE STATEMENT

Overview

5. In December 2022 and January 2023, the Rhode Island State Police (herein referred to as RISP) and the US Postal Inspection Service (herein referred to as USPIS), respectively, began operating independent investigations involving check fraud within the District of Rhode Island. In February of 2023, it was determined this was an ongoing criminal scheme and the two agencies began conducting a joint investigation that has identified Jamal Mansaray (herein referred to as MANSARAY), amongst others, as an active recruiter, facilitator, and participant in an ongoing check kiting scheme.

6. RISP began conducting their investigation on December 21, 2022, when they received notification from a Bank Newport Fraud Investigator that a \$64,763.36 check issued and mailed by the City of Taunton MA, was deposited into an account maintained by John Deasy (herein referred to as DEASY) of Tiverton, Rhode Island.

7. USPIS began their investigation on January 11, 2023, when a Santander Bank Fraud Investigator reported a \$28,142.24 check issued and mailed by the town of Norton, MA was deposited into an account maintained in the name Jessica Cabral (herein referred to as CABRAL), of Pawtucket, Rhode Island.

8. The two aforementioned checks, as well as two others issued and mailed by the town of Canton MA and Walpole MA, had been stolen from a curbside commercial mailbox used by Bi-County Collaborative (herein referred to as BICO), 397 E Central St, Franklin, MA. BICO is a special education contractor for several school districts in the area including Taunton, Norton, Canton, and Walpole. Investigators have spoken to representatives from these towns who confirmed issuing and mailing the aforementioned checks to BICO in December of 2022.¹

9. An individual matching MANSARAY's physical description was present during the deposit and withdrawal of funds associated with the DEASY/Taunton check and with the deposit of the CABRAL/Norton check.

10. Furthermore, vehicles rented by MANSARAY were present during the deposit of the CABRAL/Norton check as well as the deposit of the DEASY/Taunton check and subsequent withdrawal of funds.

11. Open source searches reveal that MANSARAY resides at the SUBJECT PREMISES. On or about February 6, 2023, law enforcement surveilled MANSARAY at the SUBJECT PREMISES. Further, investigators have confirmed that as recently as two weeks ago, MANSARAY received mail at the SUBJECT PREMISES.

DEASY / Taunton Check, Deposit

12. Information obtained from Bank Newport revealed on December 19, 2022, at 5:57 PM, check number 135128 in the amount of \$64,763.36 was deposited via the ATM at the Bank Newport branch located at 1000 Division Street, East Greenwich, RI. The check was issued by the City of Taunton MA on December 15, 2022 and drawn on account ending in 7627 maintained at Rockland Trust.

13. Investigators obtained bank surveillance video of the ATM deposit in question. A review of video from December 19, 2022, around 5:57 PM, revealed the deposit was conducted by a light-skinned male wearing a black facemask, gray sweatshirt, and sweatpants. The individual is seen

¹These towns have suffered no financial loss due to secure banking practices. However, the banks in question have suffered financial losses due to Automated Teller Machine (herein referred to as ATM) withdrawals conducted within the District of Rhode Island.

approaching the ATM on foot from the direction of an adjacent Panera Bread Restaurant. At the conclusion of the transaction, the subject is seen walking across the parking lot back toward Panera Bread. The individual in question is unknown to investigators at this time, but it was determined the individual is not DEASY.

14. Investigators obtained surveillance video from Panera Bread for December 19, 2022. Video taken from the interior of Panera Bread reveals at 5:41 PM, a heavy set, dark-skinned male, with a beard, enters Panera Bread. MANSARAY is a heavyset, dark-skinned male, with a beard. The individual was wearing a black long-sleeve Calvin Klein shirt, black pants, black boots, and a baseball hat. At 5:51 PM, the individual approached a black Honda Accord in the Panera Bread parking lot. At 5:54 PM, a second male, wearing a gray sweatshirt, and sweatpants, exited the passenger side of the black Honda Accord and walked to the aforementioned Bank Newport ATM. Several minutes later, the second male returned to the black Honda Accord and the car left the parking lot.

15. Additional video surveillance was provided by Dave's Market Place, for December 19, 2022, from 5:00PM through 7:00 PM. Dave's Market Place is located in the same plaza as the Panera and Bank Newport. This video corroborates the Panera Bread footage described above.

16. The individual captured by video inside Panera Bread and who is seen exiting and entering the driver's seat of the black Honda Accord appeared to closely resemble MANSARAY. As discussed further below, MANSARAY was renting a black Honda Accord at this time.

DEASY / Taunton Check, Withdrawals

17. All of DEASY's withdrawals and attempted withdrawals related to this case occurred on December 20, 2022. At 1:30 PM, DEASY conducted a \$14,000.00 over-the-counter cash withdrawal at the Bank Newport branch located at 5 South Angel Street, Providence, Rhode Island. Video surveillance from Bank Newport showed DEASY being dropped off at the bank in a black Honda Accord with unknown Rhode Island registration. A Flock² camera system check of black

² The Flock camera system is a nationwide network of cameras on major roadways which aids investigators in developing leads and solving crimes, it allows searches of recorded data based on vehicle make and model and allows investigators to view still images of vehicles matching search parameters.

Honda sedans in the area during this time, however, revealed a black Honda Accord bearing RI Registration 1IZ237. As noted below, such vehicle was rented to MANSARAY at this time.

18. In addition, at 1:58 PM, DEASY conducted a \$19,000.00 over-the-counter cash withdrawal at the Bank Newport branch located at 4000 Chapel View Boulevard, Cranston, Rhode Island. A FLOCK camera search revealed that the black Honda Accord bearing Rhode Island registration 1IZ237 (rented to MANSARAY at the time) exited Route 37 West on to New London Avenue toward Garden City at 1:50 PM, just eight minutes before DEASY conducted the cash withdrawal.

19. At approximately 2:36 PM, DEASY attempted to conduct a third cash withdrawal, at the Bank Newport branch located at 330 County Road, Barrington, Rhode Island. DEASY failed to conduct the withdrawal and, according to surveillance video, was turned away by the teller.

20. Video surveillance obtained by Investigators for the Providence withdrawal and attempted Barrington withdrawal shows DEASY texting on his cellular phone. Your affiant knows from training and experience, recruiters and handlers who conduct check kiting schemes often keep in constant communication with the account holders, who are attempting to withdraw funds derived from a counterfeit or reproduced checks previously deposited. In many instances, account holders are physically driven to multiple bank branches by their handlers in order to withdraw as much money as possible from the accounts into which the counterfeit or reproduced checks had been previously deposited.

Interview with DEASY

21. Investigators contacted DEASY to inquire about the above noted banking activity. DEASY claimed at first that on the day of the withdrawals, he had stopped at the Stop & Shop located at 33 West River Street, Providence, RI 02904, when he was approached in the parking lot by individuals seated in a heavily tinted Honda Accord. DEASY stated one of the individuals, a Hispanic male who was seated in the front, told DEASY to "get into the car. We know where you live. We don't want anyone to get hurt." DEASY described the male in the front seat as "Dominican," weighing approximately 220-230 pounds, approximately 5'8", and wearing a black hooded sweatshirt and a well-trimmed beard. According to DEASY, the male stated, "You have \$64,000 of our money in your business bank account, and we want it."

22. DEASY stated he proceeded to enter the Honda Accord and indicated that two additional males were in the vehicle. DEASY described the male sitting next to him in the rear as a younger-looking Hispanic male wearing a black coat and mask. DEASY described the driver as a "Dominican guy" wearing a gray windbreaker and short hair. DEASY stated his name may have been "Keith" and indicated he was not wearing a mask. One of the males provided DEASY with a deposit receipt from DEASY's bank account which indicated there was money in his account, which he placed in his pocket. DEASY has since provided this receipt to the RISP.

23. DEASY claimed he was given instructions in the event the tellers asked any questions about his cash withdrawal. DEASY was told to inform the tellers he did construction work for the City of Taunton. The check was deposited with "Allen" from the Warwick Branch.

24. DEASY stated once he completed each of the withdrawals noted above, he handed the cash to the front seat passenger. DEASY stated the males passed the money around and took pictures with their cellular phones.

25. Your affiant knows from training and experience, recruiters in check kiting schemes will often solicit individuals on various social media platforms by posting messages showing large amounts of US currency. The social media posts with pictures often solicit unsuspecting individuals by inquiring about an opportunity to earn money.

26. DEASY also stated the males appeared to be conducting telephone calls with someone on FaceTime, but indicated he was unable to see who it was.

27. DEASY stated they next drove to the Chase Bank branch at 234 Thayer Street in Providence, RI after the failed withdrawal attempt at the Bank Newport branch at 330 Country Road, Barrington RI. DEASY stated he entered the bank at approximately 3:45 PM, presented his Bank Newport card, and requested a \$7,500.00 cash advance. DEASY indicated the request was denied by the teller. DEASY stated he then met the individuals in the black Honda Accord at the Bank of America branch 271 Thayer Street, at which time DEASY was driven back to his vehicle at the Stop and Shop on West River St, Providence, RI. At the conclusion of this interview, DEASY maintained he was not involved in the fraud and wanted to pursue charges against the individuals in the Honda Accord.

28. On February 1, 2023, DEASY met with Investigators for an interview conducted at RISP Scituate Barracks. During this interview, DEASY stated he was untruthful during portions of the

previous interview. DEASY said he collaborated with the individuals who drove him around to various banks to withdraw funds. DEASY stated he was fearful for his safety and his family's safety, so he fabricated portions of his previous statements. DEASY said he contacted an individual he knew as "Keith" online to purchase cocaine. DEASY said he owed "Keith" seven hundred and fifty (\$750.00) dollars. When they met, "Keith" told DEASY in order to repay his debt, he would have to allow them to wire money to his business bank account and then withdraw the cash. DEASY stated "Keith" gave him 24 hours to decide what he was going to do, and if he refused, they would make his life hard. DEASY agreed to cooperate with the scheme and willingly gave his ATM card and pin to "Keith" and the two other males who had driven him around for the withdrawals. DEASY said he communicated with "Keith" via cellular phone and provided investigators with "Keiths" cellular phone number, which was 774-246-9417. A check of commercial data bases showed this number coming back to Omnipoint Miami E License, LLC.

29. DEASY was shown a photographic line-up of individuals which included a DMV photo of MANSARAY. After reviewing the line-up, DEASY stated he was "50/50" sure that the individual he knew as "Keith" (the driver of the Honda Accord) was pictured in the photo lineup. DEASY indicated "Keith" was the person in the photo known to be MANSARAY.

Mansaray's Car Rentals

30. According to documents obtained by investigators, MANSARAY³ initially rented a black Honda Accord, RI registration 1IZ237, for the period December 18, 2022 through December 25, 2022 from Car Rentals RI, LLC.

31. Despite initially renting the Accord from December 18 through December 25, 2022, MANSARAY returned the Honda Accord early, on December 20, 2022, at approximately 4:30 PM.

32. While returning the Honda Accord, MANSARAY rented a 2011 silver Ford Explorer, RI registration 1HD892, which he returned on January 1, 2023. Your affiant knows from training and

³ The rental application for the Honda Accord bearing Rhode Island registration 1IZ237 listed MANSARAY's Rhode Island license number, phone number ending -9438, and Progressive insurance card bearing policy ending in #8254.

experience individuals involved in check kiting schemes will rent vehicles, and in some instances, multiple vehicles at the same time, in an effort to hinder investigators and obscure their true identity and nefarious activities.

33. On the same day that MANSARAY switched his rental vehicles, DEASY conducted both the DEASY/Taunton check withdrawals and the CABRAL/Norton check deposit. Further, MANSARAY's car exchange was conducted only 30 minutes after DEASY was dropped off at the Stop & Shop on West River Ave. in Providence, RI, and approximately three hours before the CABRAL/Norton deposit was conducted.

CABRAL / Norton Check

34. Information obtained from Santander Bank revealed on December 20, 2022, at 7:16 PM, check number 109530, in the amount of \$28,142.24, was deposited at the Santander Bank ATM located at 280 Atwells Avenue, Providence, RI. The check was issued on December 15, 2022, by the City of Norton, MA and was drawn on this account maintained at UniBank.

35. Investigators obtained bank surveillance video of the above-mentioned ATM deposit. A review of the surveillance video shows the check was deposited by a heavy-set male, either dark-skinned Hispanic or light-skinned African American. The suspect is shown wearing a mask which obscured his face, a distinct hooded sweatshirt with a shark logo, khaki pants, sneakers, and a New York Yankees baseball hat. The individual can clearly be seen using his cellular phone before and during the ATM deposit. The individual was not the account holder (CABRAL), who is a female.

36. Investigators obtained surveillance video from the exterior of the Santander Bank ATM located on Atwells Avenue for December 20, 2023, for the period between 7:00 PM and 7:30 PM. The video footage showed a silver Ford Explorer traveling east on Atwells Avenue at 7:13 PM, (approximately three minutes before the CABRAL/Norton check was deposited at Santander Bank). The footage also showed the Explorer entering the parking lot next to the Santander Bank located at the corner of Atwells Avenue and DePasquale Avenue, Providence, RI. Shortly after the vehicle was parked, the aforementioned individual is seen exiting the vehicle and walking toward the entrance of the bank. The silver Ford Explorer was of particular interest because it is the same make and model vehicle MANSARAY rented on December 20, 2022, after returning the Honda Accord used in conducting the Bank Newport deposit of the DEASY/Taunton check.

CI-1 Interview

37. On Friday March 17, 2023, at approximately 0930 hours RISP Detective and US Postal Inspectors spoke with a confidential informant, CI-1.⁴ This conversation took place in Cranston, RI at the Intake Center for the Rhode Island Department of Corrections. CI-1 was told that the conversation was completely voluntary, and he was free to leave the company of investigators at any time and not to say anything to investigators if he chose not to. CI-1 agreed to stay and speak with Investigators.

38. CI-1 was asked about fraudulent check schemes in the District of Rhode Island. CI-1 said he knew an individual who went by the nick name “MONSSIE” (unknown spelling, spelled phonetically) who was involved with fraudulent checks. CI-1 stated he knew MONSSIE to possess and distribute counterfeit or reproduced checks, most of which were stolen from the US Mail. CI-1 explained this was done because the checks could be deposited into other individuals’ bank accounts then the funds withdrawn without directly implicating MONSSIE in the transactions. CI-1 went on to say the money withdrawn was then given back to MONSSIE and a small fee was paid to the depositor whose account was used. CI-1 said he only deposited counterfeit or reproduced checks that he received from MONSSIE and that he did this four or five times, including on the dates of August 29, 2022 and December 6, 2022.

39. CI-1 stated the individual he knew as MONSSIE would frequently operate different vehicles. CI-1 stated he never saw the individual he knew as MONSSIE with any other individuals in his vehicle. CI-1 stated he would get in touch with the individual he knew as MONSSIE through Facebook Messenger or other electronic messaging applications over his cellular phone. CI-1 stated he never went to MONSSIE’s house, and when they met it would be in a parking lot somewhere in the Providence or surrounding area.

40. CI-1 was shown a photo and identified the individual in that photo as the person he knew as MONSSIE; the photo was of MANSARAY. CI-1 was shown other photos of the individuals

⁴ CI-1 has provided the RISP with information regarding check fraud investigations on one occasion since approximately March 17, 2023. CI-1 has a criminal history that includes Obtaining Money by False Pretenses, Fraudulent Checks over \$1500, Forgery and Counterfeiting, Larceny over \$1500, Domestic Disorderly, Domestic Simple Assault, Obstructing Officer in Execution of Duty, License or Permit Required for Carrying a Pistol, Possession of Arms by a Convict, and Conspiracy.

depositing the checks stolen from BICO, in December of 2022; he stated he did not know any of the individuals.

EVIDENCE OBTAINED DURING RESIDENTIAL SEARCHES

41. Based on my training and experience, I know that during the course of residential searches, I and other Inspectors and agents have found items of personal property that tend to identify the person(s) in residence, occupancy, control, or ownership of the subject premises and electronic devices located therein. Such identification evidence is typical of the articles people commonly maintain in their residences, such as canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, utility and telephone bills, statements, identification documents, and keys.

42. Given the nature of this crime, it is reasonable to believe that access devices used in check fraud schemes, such as debit cards, checks, bank account information and information relating thereto (names, passwords, online user log ins, etc.) would be maintained in a place that allowed for safe storage, but ready access, such as a residence, for creation of fraudulent checks and use for access to accounts.

EVIDENCE RELATING TO FRAUD OFFENCES

43. Based on my training and experience and familiarity with investigations into fraud conducted by other law enforcement agents, I know the following:

- a. Individuals maintain in their homes, both in paper and electronic format, among other items, records regarding the receipt and expenditure of money, documents relating to the purchase of assets, and records pertaining to their employment or business, even if that business is an illicit business.
- b. Given the nature of fraud, I believe that participants in a long running fraud that involves several participants, more often than not, will keep records containing names, addresses, email addresses, social media accounts, and telephone numbers

of co-conspirators, as well as targets, victims, and those used to perpetrate the fraud, amounts received from them, and amounts sent to third parties. These records are necessary to further the illicit fraud business and can be found in paper form or stored electronically in cell phones and other electronic devices.

- c. I also know that those who make use of stolen personal identification as part of their fraud schemes, will often keep lists of the stolen PII, and notations on how and when that identify may be used, and any passwords for that “identity.” I am also aware that fraudsters often maintain such documents related to their criminal activities at their residences or other locations over which they have control for an extended period of time, due to the high value associated with stolen PII that has been successfully used.
- d. From training and experience, I know that individuals who amass proceeds from illegal activities routinely attempt to further that conduct and/or conceal the existence and source of their funds by engaging in financial transactions with domestic and foreign institutions, and others, through all manner of financial instruments, including cash, USPS Money Orders, cashier’s checks, credit and debit cards, money drafts, traveler’s checks, wire transfers, etc. Records of such instruments, including ATM receipts, are oftentimes maintained at the individual’s residence.
- e. There are many reasons why criminal offenders maintain evidence for long periods of time. First, to the offender, the evidence may seem innocuous at first glance (e.g. financial, credit card and banking documents, travel documents, receipts, documents reflecting purchases of assets, personal calendars, telephone and address directories, checkbooks, videotapes and photographs, utility records, ownership records, letters and notes, tax returns and financial records, escrow files, telephone bills, keys to safe deposit boxes, packaging materials, computer hardware and software). To law enforcement, however, such items may have significance and relevance when considered in light of other evidence. Second, the criminal offender may no longer realize he/she still possesses the evidence or may believe law enforcement could not obtain a search warrant to seize the evidence. The criminal

offender may also be under the mistaken belief that he/she has deleted, hidden or further destroyed electronic/computer-related evidence, which in fact, may be retrievable by a trained forensic computer expert. Thus, records and ledger-type evidence that one would think a prudent person might destroy because of its incriminatory nature are sometimes still possessed months or even years after the records were created.

- f. Based on my knowledge with respect to facts and circumstances in this investigation, as well as my experience and training relating to cases involving individuals engaged in fraud schemes, as well as my discussions with other Inspectors and agents who investigated such cases, I know that it is a common practice for individuals engaged in these illegal activities to maintain the items and records or documents as set forth in Attachment B, whether maintained on paper, in hand-written, typed, photocopied, or printed form, or electronically on a computer or cell phone, hard disks, external drives, RAM, flash memory, CD-ROMS, memory sticks, USB drives, and other magnetic or optical media, or any other storage medium.

TRAINING AND EXPERIENCE ON DIGITAL DEVICES

44. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

- a) Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b) Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c) The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d) Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

45. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a) Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b) Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

46. The search warrant also requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a) Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b) In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c) Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress the user's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of the user's face with her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

d) Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

REQUEST FOR SEALING

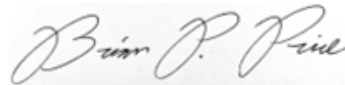
47. Because this investigation is continuing and disclosure of some of the details of this affidavit may cause the targets or other affiliated persons to flee or further mask their identity or activities, destroy physical and/or electronic evidence, or otherwise obstruct and seriously jeopardize this investigation, I respectfully request that this affidavit, and associated materials seeking this search warrant, be sealed until further order of this Court. Finally, I specifically request that the sealing order not prohibit information obtained from this warrant from being shared with other law enforcement and intelligence agencies.

CONCLUSION

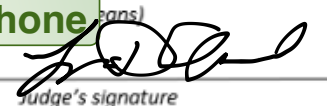
48. Based on all the foregoing facts, I submit that there is probable cause to believe that the items to be seized described in Attachment B will be found in a search of the SUBJECT PERSON and SUBJECT PREMISES described in Attachments A-1 and A-2, respectively.

Sworn under the pains and penalties of perjury.

Respectfully submitted,



Brian P. Prive
United States Postal Inspector
United States Postal Inspection Service

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by _____ (specify means)	
Date May 25, 2023	 Judge's signature
Providence RI City and State	Magistrate Judge Lincoln D. Almond

ATTACHMENT A-1

PERSON TO BE SEARCHED / SUBJECT PERSON

The person identified as JAMAL MANSARAY, YOB 1989, SSN ending -2131 last known address of 180 Waterman Avenue, Apartment [REDACTED] North Providence, Rhode Island 02911 (SUBJECT PERSON), pictured below, at whatever location he is found, including any computers, cellular telephones, cellular and digital devices, digital storage devices or other storage media/medium, briefcases, backpacks, wallets, and purses, he may have on his person.



ATTACHMENT A-2

ADDRESS TO BE SEARCHED / SUBJECT PREMISES

180 Waterman Avenue, Apartment Number [REDACTED], North Providence, Rhode Island 02911 (SUBJECT PREMISES), pictured below. The complex is 150 loft-style apartments, known as Greystone Lofts.



ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as a means of committing a criminal offense, namely violations of 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1344 (bank fraud), 18 U.S.C. § 1029 (access device fraud), 18 U.S.C. § 1028A (aggravated identify theft), and 18 U.S.C. § 1708 (theft or receipt of stolen mail matter) (“Specified Federal Offenses”):

1. Records, information, and items relating to the acquisition, alteration, and/or creation of checks for accounts in the names of third persons or companies.
2. Records, information, and items relating to acquisition and use of personally identifiable information (“PII”) of third parties, including but not limited to names, bank account numbers, ATM numbers, PIN numbers.
3. Records, information, and items relating to acquisition and use of debit cards in the names of third persons.
4. Records, information, and items relating to the opening of, use, and access of bank accounts in the names of third persons, and any and all bank statements, transaction records, and ATM receipts for such accounts.
5. Records, information, and items relating to the deposit of checks for accounts in the names of third persons or companies, and attempts to withdraw and withdrawal of proceeds of those checks.
6. Records, information, and items relating to any communications by, between and among, and/or relating to the SUBJECT PERSON and known and unknown conspirators and witting or unwitting accomplices, relating to the Specified Federal Offenses, via any social media, online account, and communications platforms, including but not limited to Snapchat, Instagram, Facebook, Facebook Messenger, Pinterest, FaceTime, Skype, email, telephone, and any SMS and MMS messaging platforms, including WhatsApp and Telegram.
7. Records, information, and items relating to the recruitment or solicitation of persons to assist in the cashing of checks provided by the SUBJECT PERSON, and offers to pay or payments for recruitment.
8. Records, information, and items relating to banking and financial accounts and records of or relating to the SUBJECT PERSON, and known and unknown co-conspirators and witting or unwitting accomplices, used in furtherance of the Specified Federal Offenses, and known and unknown conspirators, and their nominees, assignees, including bank statements, deposit tickets, deposit items, checks, money orders, cashier’s checks, official checks, bank drafts, wire transfer instructions and receipts, checkbooks, check registers, passbooks, withdrawal slips, credit memos, debit memos, signature cards, account applications, automatic teller machine receipts, safe deposit box applications, safe deposit box keys, pre-paid debit and credit cards, debit and credit card statements, charge slips, receipts, financial statements, balance sheets, income statements, cash flow statements,

ledgers, journals, accounts receivable, accounts payable, leases, brokerage statements, and any other items evidencing the obtaining, disposition, secreting, transfer, or concealment of assets.

9. Records, information, and items relating to the access and use of money service businesses, such as Western Union and/or Moneygram; online bank transfer services, such as Zelle, Venmo, Cash App, or Paypal; and cryptocurrency accounts and cryptocurrency exchanges, such as Bitcoin.
10. United States currency, money orders or cashier's checks.
11. Records, information, and items relating to Global Positioning System ("GPS") coordinates and use of GPS mapping systems that identify persons, places, and information that constitute evidence of the commission the Specified Federal Offenses.
12. Records, information, and items records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators and witting or unwitting accomplices, involved in the Specified Federal Offenses, including calendars, address books, telephone or other contact lists, correspondence, receipts, and wire transfer or fund disposition records, and communications relating to the same.
13. Records, information, and items concerning occupancy, ownership, purchase and/or lease of the SUBJECT PREMISES (180 Waterman Avenue, Apartment [REDACTED], North Providence, Rhode Island 02911), and prior addresses of the SUBJECT PERSON.
14. Records, documents, and deeds reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry, or other items obtained with fraud proceeds.
15. Identification cards, driver's license cards, passports, visas, and travel documents.
16. Records, information, and items relating to the use, ownership, possession, and control of computers, tablets, cellular telephones, and/or other cellular and digital devices seized from the SUBJECT PREMISES and/or any person located therein; seized from the SUBJECT PERSON; and any landline telephones, internet service, or IP addresses associated with the SUBJECT PREMISES.
17. For any computer, cellular or digital device, cellular telephone, and/or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information whose seizure is

authorized by this warrant, including any cell phones (hereinafter, "DIGITAL DEVICE")⁵:

- a. evidence of who used, owned, or controlled the DIGITAL DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the DIGITAL DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crimes under investigation and to the computer user;
- e. evidence indicating the computer user's knowledge and/or intent as it relates to the crimes under investigation;
- f. evidence of the attachment to the DIGITAL DEVICE of other storage devices or similar containers for electronic evidence;
- g. evidence of programs (and associated data) that are designed to eliminate data from the DIGITAL DEVICE;
- h. evidence of the times the DIGITAL DEVICE was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the DIGITAL DEVICE;
- j. documentation and manuals that may be necessary to access the DIGITAL DEVICE or to conduct a forensic examination of the DIGITAL DEVICE;
- k. records of or information about Internet Protocol addresses used by the DIGITAL DEVICE; and
- l. records of or information about the DIGITAL DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

18. Routers, modems, and network equipment used to connect computers to the Internet.

⁵ The term "DIGITAL DEVICE" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile/cellular phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, external drives, RAM, flash memory, CD-ROMS, memory sticks, USB drives, and other magnetic or optical media.

19. With respect to any and all electronically stored information in cellular telephones and cellular devices, in addition to the information described herein, Inspectors and agents may also access, record and seize the following information to the extent that it identifies persons, places, and information that constitute evidence of the commission the Specified Federal Offenses:
- a. Telephone numbers of incoming/outgoing calls stored in the call registry;
 - b. Digital, cellular and/or telephone numbers and/or direct connect numbers, names and identities stored in the directories;
 - c. Any incoming/outgoing text messages relating to the above criminal violations;
 - d. Telephone subscriber information;
 - e. The telephone numbers stored in the cellular telephone and/or PDA;
 - f. Records relating to the use, possession, and control of any cellular telephones and cellular devices seized;
 - g. Any other electronic information stored in the memory and/or accessed by the active electronic features of the digital or cellular telephone including photographs, videos, e-mail, and voice mail relating to the above Specified Federal Offenses.
20. Any and all opened or sealed USPS or other mail envelopes and packages, to include but not limited to such envelopes and packages from individuals identified as victims in this investigation and more generally, in relation to any counterfeit check scheme and/or the transfer and receipt of funds between the subjects of the investigation and other persons;
21. Clothing worn by the SUBJECT PERSON during the deposits or withdrawals of any of the checks or funds in question;
22. Contextual information necessary to understand the evidence described in this attachment.

AUTHORIZED SEARCH PROCEDURE

1. Law enforcement personnel or other individuals assisting law enforcement personnel (the “search team”) will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location.
2. In order to search for the items described above that may be maintained in electronic media, the search team are authorized to search, copy, image and seize the following items for off-site review:

- a. Any computer or storage medium capable of being used to commit further or store evidence of the Specified Federal Offenses; and
 - b. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer or storage medium;
3. Pursuant to Rule 41(f)(1)(B), the government will retain a copy of the electronically stored information that was seized or copied for the purpose of the evidentiary authentication and any potential discovery obligations in any related prosecution.

SEARCH PROCEDURE FOR DEVICES CAPABLE OF BIOMETRIC ACCESS

1. During the execution of this search warrant, law enforcement is permitted to:
 - a. depress the SUBJECT PERSON's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and
 - b. hold the device in front of the SUBJECT PERSON's face with her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.